REMARKS

The Examiner is thanked for the careful review of this application.

Favorable reconsideration and allowance of the present patent application are respectfully requested in view of the foregoing amendments and the following remarks. Claims 1-4, 6-8, 10-15 and 17-25 are pending in the current application. Claims 1, 10, 11, 18, and 19 are independent claims.

Claim Objections

Claim 8 is objected to for including a minor informality, which has been addressed by this Amendment. Accordingly, the Applicants respectfully request that the Office withdraw this objection.

Rejection under 35 U.S.C. §103(a) over Koskimies in view of Bilange

Claims 1-4, 6-7, 10-14 and 17-24 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Publication No. 2004/0081110 ("Koskimies") in view of U.S. Publication No. 2004/0093595 ("Bilange"). The Applicants respectfully traverse this art ground of rejection.

As described at [0079]-[0080] of Koskimies, a secret code is generated for the target device and is made available to the target device and the trusted download server (or data storage system) that is providing the content. Then, the requested content from the trusted download server is encrypted and can only be decrypted by the target device via the use of the secret code (e.g., [0079]-[0081] of Koskimies). Therefore, Koskimies states that "[s]ince content will only work with a single target device, copying the content is of no use" (e.g., [0083] of Koskimies).

The requested content is conveyed to the target device from the content server via an SMS or text message (e.g., see [0065] of Koskimies).

The Office cites to [0044]-[0046] of Bilange for allegedly curing Koskimies failure to disclose "wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment" (e.g., see Page 4 of the Office Action). However, the Applicants have reviewed the cited section of Bilange and respectfully submit that Bilange actually operates in a very similar manner as Koskimies and includes the same deficiencies.

As noted above, the secret code in Koskimies is used to control whether the target device can decrypt the encrypted content (e.g., [0079]-[0081] of Koskimies). Compare this aspect of Koskimies with Bilange's discussion of the "unlock code" as follows:

> ... the application provisioning server takes control of the registered application on first launch to get an unlock code that will be stored on the mobile device for subsequent launches. The unlock code may be provided to the device when the application is initially downloaded. Because the unlock code cannot be copied from one mobile device to another, this prevents the execution of unauthorized copies of the registered application and is done as an additional security measure against piracy... *(e.g., [0046] of Bilange)*

Accordingly, the security protocol used by Koskimies is based on the presence of the secret code for decrypting the content, and the security protocol used by Bilange is based on the presence of the unlock code that is used for each launch of an application on a mobile device. In both Koskimies and Bilange, no access appears to be permitted for "downloaded applications that do not comply with the predefined security", i.e., applications that do not have the requisite code.

Further, the Applicants note that Bilange discusses two different software platforms or application execution environments (e.g., J2ME and WAP). However, the WAP browser, which

runs under a Wireless Application Environment (WAE), simply appears to be an example mechanism for downloading J2ME-compliant applications. For example, Bilange states that "a registered application can be implemented in a J2ME environment, where the top-level application is called a MIDlet" (e.g., [0015]), "[t]he registered applications may be discovered through the mobile device's WAP browser (not shown), provided that the registered applications are compatible with the user's specific mobile device" (e.g., [0034]), "[m]any mobile devices conform to J2ME guidelines and recommended practices for user-initiated OTA provisioning and MIDP provisioning in the WAP environment and use the WAP browser to initiate download" (e.g., [0035]), "the download may be initiated from WAP" (e.g., [0045]), etc.

Thus, in Bilange, the WAP browser is just a mechanism for downloading the J2ME applications or MIDlets. Once downloaded, the J2ME applications are simply executed in the J2ME environment (assuming the mobile device has the requisite unlock code). Thus, the only execution environment for downloaded J2ME applications in Bilange is the J2ME environment. There is no disclosure that some other environment would be used for the execution of non-secure J2ME applications, in other words. Again, the strong implication in Bilange is that non-secure applications (or applications without an unlock code) would be blocked from execution altogether.

In view of the above-remarks, the Applicants respectfully submit that the combination of Koskimies and Bilange fails to disclose or suggest "wherein the selectively downloaded applications that comply with the predefined security protocol are executed by the computer platform within the resident application environment" and "wherein the selectively downloaded applications that do not comply with the predefined security protocol are executed by the download manager outside of the resident application environment" as recited in independent claim 1 and similarly recited in independent claims 10, 11, 18 and 19.

As such, claims 2-4, 6-7, 12-14, 17 and 20-24, dependent upon independent claims 1, 11, 18 and 19, respectively, are likewise allowable over Koskimies in view of Bilange at least by virtue of their dependence upon the independent claims.

The Applicants respectfully request that the Office withdraw this art grounds of rejection.

Rejection under 35 U.S.C. §103(a) over Koskimies in view of Bilange in view of Hericourt

Claims 8, 15 and 25 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Koskimies") in view of Bilange in further view of U.S. Patent No. 7,099,916 ("Hericourt"). The Applicants respectfully traverse this art ground of rejection.

As an initial matter, the Applicants agree with the Office's admission that Koskimies and Bilange fail to disclose features specific to dependent claims 8, 15 and 25 (e.g., see Pages 13-15 of the Office Action). The Office alleges that Hericourt cures these particular deficiencies of Koskimies and Bilange. Hericourt is directed to a system and method for downloading a virus-free file certificate from a file server, whereby the file certificate is provided to a requesting entity to verify that a certificate is virus-free (e.g., Hericourt, Abstract). Even assuming for the sake of argument that Hericourt discloses the features specific to claims 8, 15 and 25 (which the Applicants do not admit), the Applicants respectfully submit that a review of Hericourt indicates that Hericourt is insufficient to cure the suggestion and disclosure deficiencies of Koskimies and/or Bilange as discussed above with respect to independent claims 1 and 11.

As such, claims 8, 15 and 25, dependent upon independent claims 1 and 11, respectively, are likewise allowable over Koskimies in view of Bilange in view of Hericourt at least by virtue of their dependence upon the independent claims.

Further, by adding claim 25, the Applicants attempted to show that the Koskimies (and now Bilange) are exclusively concerned with piracy. In other words, the secret code in

Koskimies and the unlock code in Bilange is not a security mechanism to protect the device executing the software, but rather to protect the owner of the application from unauthorized executions, which is a fundamentally different type of security. It is true that Hericourt is related to device security, because Hericourt relates to an anti-virus program. However, while some type of anti-virus program could certainly be added to the J2ME environment in Koskimies or Bilange, the Applicants do not believe that it makes sense to combine Hericourt with Koskimies or Bilange such that the trusted code or secret code would become part of an anti-virus scheme. Such a combination would imply that the trusted code or secret code would be used to verify a virus-free application instead of verifying permission to use an application. There is simply no rationale that the Applicants can find for making such a change to Koskimies and/or Hericourt. So long as the Office reads the "predefined security protocol" on a permission-to-use security scheme in Koskimies and Bilange, the Applicants believe it unreasonable to then cite to Hericourt to suggest that the operation of Koskimies and Bilange would be switched to an anti-virus scheme. For this reason, there is no apparent reason for Hericourt to be combined with Koskimies and/or Bilange to achieve "wherein the predefined security protocol is configured to protect the computer device". Rather, any anti-virus program added to Koskimies and/or Bilange would likely run separate from the permission-to-use security schemes presented in Koskimies and/or Bilange.

The Applicants respectfully request that the Office withdraw this art grounds of rejection.

CONCLUSION

In light of the remarks and/or amendments contained herein, the Applicants respectfully submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated August 5, 2011

By: /Fariba Yadegar-Bandari/
Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502